Fiscal Year 2017

Senior Agency Official for Privacy Federal Information Security Modernization Act of 2014 Reporting Metrics v1.0

1 September 2017

Document History

Version	Date	Comments	See/Page
1.0	1 September 2017	Final FY 2017 SAOP FISMA Metrics	All

Contents

1 Information Systems

1a. Number of Federal information systems[1] reported in response to question 1.1 of the FY 2017 Chief Information Officer FISMA Metrics that are used to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information (PII).[2]

1b. Number of information technology[3] (IT) systems maintained, operated, or used by the agency (or by another entity on behalf of the agency) for which the agency is required to conduct a privacy impact assessment (PIA) under the E-Government Act of 2002.

1c. Number of IT systems reported in question 1b that are covered by an up-to-date PIA.[4]

1d. Number of Privacy Act systems of records[5] maintained by the agency (including those operated by a contractor on behalf of the agency).

1e. Number of Privacy Act systems of records reported in question 1d for which an up-to-date system of records notice (SORN) has been published in the *Federal Register*.[6]

2 General Requirements

2a. Has the head of the agency designated an SAOP and reported the name, title, and contact information of the current SAOP to OMB on the MAX website of the Federal Privacy Council?[7]

2b. Does the SAOP have the necessary position, expertise, and authority to serve in the role of SAOP?[8]

2c. Does the SAOP have the necessary role in the agency's policy making, compliance, and risk management activities?[9]

2d. Has the agency developed and maintained a privacy program plan?[10]

2e. Does the agency maintain an inventory of the agency's websites, applications, social media accounts, and other digital services?

2f. Does the agency maintain and post privacy policies on all agency websites, mobile applications, and other digital services, in accordance with the E-Government Act of 2002 and OMB policy?[11]

2g. Has the agency developed and implemented a process to regularly review and update the privacy policies for each of the agency's websites, mobile applications, and digital services?

2h. Has the agency developed and implemented a written policy or procedure for the agency's use of social media (indicate "N/A" if the agency does not use social media)?

2i. During the reporting period, did the agency use web management and customization technologies on any website or mobile application?[12]

2j. During the reporting period, did the agency review the use of web management and customization technologies to ensure compliance with all laws, regulations, and OMB guidance (indicate "N/A" if the agency does not use web management and customization technologies)?[13]

3 Considerations for Managing PII

3a. Does the agency maintain an inventory of the agency's information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII?[14]

3b. Does the agency ensure, to the extent reasonably practicable, that PII created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed of is accurate, relevant, timely, and complete?[15]

3c. Does the agency limit the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII to that which is legally authorized, relevant, and reasonably deemed necessary for the proper performance of agency functions?[16]

3d. Does the agency have an inventory of the agency's collection and use of Social Security numbers (SSNs)?[17]

3e. Does the agency maintain the inventory of SSNs as part of the agency's inventory of information systems referred to in question 3a (indicate "N/A" if the agency does not have an inventory of its collection and use of SSNs)?

3f. Has the agency developed and implemented a written policy or procedure to ensure that any new collection or use of SSNs is necessary?

3g. Does the written policy or procedure referred to in question 3f provide specific criteria to use when determining whether the collection or use of SSNs is necessary (indicate "N/A" if the agency does not have a written policy or procedure)?

3h. Does the written policy or procedure referred to in question 3f provide specific steps to ensure that any collection or use of SSNs associated with agency websites, online forms, mobile applications, and other digital services, is necessary and complies with applicable privacy requirements (indicate "N/A" if the agency does not have a written policy or procedure)?

3i. Does the written policy or procedure referred to in question 3f establish a process to ensure that any necessary collection or use of SSNs remains necessary over time (indicate "N/A" if the agency does not have a written policy or procedure)?

3j. Has the agency taken steps during the reporting period to eliminate the unnecessary collection and use of SSNs (indicate "N/A" if the agency has successfully eliminated all unnecessary collections and uses of SSNs at the agency)?[18]

4 Budget and Acquisition

4a. Does the agency identify and plan for the resources needed to implement the agency's privacy program?[19]

4b. Does the agency have a process that includes explicit criteria for analyzing privacy risks when considering IT investments?[20]

4c. During the reporting period, did the agency review IT capital investment plans and budgetary requests to ensure that privacy requirements (and associated privacy controls), as well as any associated costs, were explicitly identified and included, with respect to any IT resources that will be used to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII?[21]

4d. Does the agency plan and budget to upgrade, replace, or retire any information systems that maintain PII for which protections commensurate with risk cannot be effectively implemented?[22]

4e. Does the agency ensure that, in a timely manner, the SAOP is made aware of information systems and components that cannot be appropriately protected or secured?[23]

5 Contractors and Third Parties

5a. Does the agency ensure that terms and conditions in contracts, and other agreements involving the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of Federal information, incorporate privacy requirements and are sufficient to enable agencies to meet Federal and agency-specific requirements pertaining to the protection of Federal information?[24]

5b. Does the agency, consistent with the agency's authority, ensure that the requirements of the Privacy Act apply to a Privacy Act system of records when a contractor operates the system of records on behalf of the agency to accomplish an agency function?[25]

5c. Does the agency document and implement policies and procedures for privacy oversight of contractors and other entities, to include ensuring appropriate vetting and access control processes for contractors and others with access to information systems containing Federal information?[26]

5d. Does the agency develop, maintain, and implement mandatory agency-wide privacy awareness and training programs for all contractors?[27]

6 Privacy Impact Assessments

6a. Has the agency developed and implemented a written policy or procedure for determining whether a PIA is required when the agency develops, procures, or uses an IT system?[28]

6b. Has the agency developed and implemented a written policy or procedure to ensure that a PIA is conducted and approved before an IT system that requires a PIA is developed, procured, or used?[29]

6c. Has the agency developed and implemented a written policy or procedure for assessing the quality and thoroughness of each PIA and performing reviews to ensure that appropriate standards for PIAs are maintained?[30]

6d. Has the agency developed and implemented a written policy or procedure to ensure that system owners, privacy officials, and IT experts participate in conducting the PIA?[31]

6e. Has the agency developed and implemented a written policy or procedure for monitoring the agency's IT systems and practices to determine when and how PIAs should be updated?[32]

6f. Has the agency developed and implemented a written policy or procedure to ensure that PIAs are updated whenever a change to an IT system, a change in agency practices, or another factor alters the privacy risks?[33]

7 Workforce Management

7a. Does the agency ensure that the agency's privacy workforce has the appropriate knowledge and skill?[34]

7b. Is the SAOP involved in assessing the hiring, training, and professional development needs of the agency with respect to privacy?[35]

7c. Has the SAOP participated in developing and maintaining a current workforce planning process?[36]

7d. Has the SAOP participated in developing a set of competency requirements for privacy staff, including program managers and privacy leadership positions?[37]

8 Training and Accountability

8a. Has the agency developed, maintained, and implemented mandatory agency-wide privacy awareness and training programs for all employees?[38]

8b. Has the agency provided foundational as well as more advanced levels of privacy training for information system users (including managers, senior executives, and contractors) during the reporting period?[39]

8c. Has the agency ensured that measures are in place to test the knowledge level of information system users in conjunction with privacy training?[40]

8d. Has the agency provided role-based privacy training during the reporting period for employees and contractors with assigned privacy roles and responsibilities, including managers, before authorizing access to Federal information or information systems or performing assigned duties?[41]

8e. Has the agency developed and implemented policies and procedures to ensure that all personnel are held accountable for complying with agency-wide privacy requirements and policies?[42]

8f. Has the agency established rules of behavior, including consequences for violating rules of behavior, for employees and contractors that have access to Federal information or information systems, including those that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII?[43]

8g. Does the agency ensure that employees and contractors have read and agreed to abide by the rules of behavior for the Federal information and information systems for which they require access prior to being granted access (indicate "N/A" if the agency does not have established rules of behavior)?[44]

9 Incident Response

9a. Does the agency have a breach response plan that includes the agency's policies and procedures for reporting, investigating, and managing a breach?[45]

9b. Did the SAOP review the agency's breach response plan during the reporting period to ensure that the plan is current, accurate, and that it reflects any changes in law, guidance, standards, agency policy, procedures, staffing, and/or technology (indicate "N/A" if the agency does not have a breach response plan)?[46]

9c. Does the agency have a breach response team composed of agency officials designated by the head of the agency that may be convened to lead the agency's response to a breach?[47]

9d. Did all members of the agency's breach response team participate in at least one tabletop exercise during the reporting period (indicate "N/A" if the agency does not have a breach response team)?[48]

9e. How many breaches, as the term "breach" is defined in OMB Memorandum M-17-12, were reported within the agency during the reporting period?[49]

9f. How many breaches did the agency's principal security operations center report to the DHS United States Computer Emergency Readiness Team (US-CERT) during the reporting period?[50]

9g. How many breaches did the agency report to Congress during the reporting period?[51]

9h. What is the total number of individuals potentially affected by the breaches reported in question 9g (indicate "N/A" if the agency did not report a breach to Congress during the reporting period)?[52]

10 Risk Management Framework

10a. Has the agency implemented a risk management framework to guide and inform the categorization of Federal information and information systems; the selection, implementation, and assessment of privacy controls; the authorization of information systems and common controls; and the continuous monitoring of information systems?[53]

10b. Does the SAOP review and approve, in accordance with NIST FIPS Publication 199 and NIST Special Publication 800-60, the categorization of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII?[54]

10c. Has the SAOP designated which privacy controls will be treated as program management, common, information system-specific, and hybrid privacy controls at the agency?[55]

10d. Has the agency developed and maintained a privacy plan, reviewed and approved by the SAOP, for agency information systems prior to authorization, reauthorization, or ongoing authorization?[56]

10e. Does the SAOP conduct and document the results of privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented at the agency across all agency risk management tiers to ensure continued compliance with applicable privacy requirements and manage privacy risks?[57]

10f. Has the SAOP developed and maintained a written privacy continuous monitoring strategy?[58]

10g. Has the SAOP established and maintained an agency-wide privacy continuous monitoring program?[59]

10h. Does the SAOP review authorization packages for information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII to ensure

compliance with applicable privacy requirements and manage privacy risks, prior to authorizing officials making risk determination and acceptance decisions?[60]

11 Privacy Act

11a. Has the agency developed and implemented a written policy or procedure for determining whether a SORN is required when the agency collects or maintains information?[61]

11b. Has the agency developed and implemented a written policy or procedure for ensuring that information collections include a Privacy Act Statement, if required?[62]

11c. Has the agency developed and implemented a written policy or procedure for receiving, processing, and responding to individuals' requests for access to and amendment of records?[63]

11d. Has the agency selected, implemented, assessed, and monitored privacy controls for information systems that contain information in a system of records in order to ensure that no system of records includes information about an individual that is not relevant and necessary to accomplish a purpose required by statute or executive order?[64]

11e. Has the agency selected, implemented, assessed, and monitored privacy controls for information systems that contain information in a system of records in order to ensure that all SORNs remain accurate, up-to-date, and appropriately scoped; that all SORNs are published in the *Federal Register*; that all SORNs include the information required by OMB Circular A-108; and that all significant changes to SORNs have been reported to OMB and Congress?[65]

11f. Has the agency selected, implemented, assessed, and monitored privacy controls for information systems that contain information in a system of records in order to ensure that all routine uses remain appropriate and that the recipient's use of the records continues to be compatible with the purpose for which the information was collected?[66]

11g. Has the agency selected, implemented, assessed, and monitored privacy controls for information systems that contain information in a system of records in order to ensure that each exemption claimed for a system of records pursuant to 5 U.S.C. § 552a(j) and (k) remains appropriate and necessary?[67]

11h. Has the agency selected, implemented, assessed, and monitored privacy controls for information systems that contain information in a system of records in order to ensure that the language of each contract that involves the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal of information that identifies and is about individuals, is sufficient and that the applicable requirements in the Privacy Act and OMB policies are enforceable on the contractor and its employees?[68]

11i. Has the agency selected, implemented, assessed, and monitored privacy controls for information systems that contain information in a system of records in order to ensure that the agency's training practices are sufficient and that agency personnel understand the requirements of the Privacy Act, OMB guidance, the agency's implementing regulations and policies, and any job-specific requirements?[69]

12 Privacy Program Website

12a. Does the agency have a Privacy Program Page located at www.[agency].gov/privacy?[70]

12b. Does the agency's Privacy Program Page include a list and provide links to complete, up-to-date versions of all agency SORNs?[71]

12c. Does the agency's Privacy Program Page include a list and provide links to PIAs?[72]

12d. Does the agency's Privacy Program Page include a list and provide links to up-to-date matching notices and agreements for all active matching programs in which the agency participates?[73]

12e. Does the agency's Privacy Program Page include citations and provide links to the final rules published in the *Federal Register* that promulgate each Privacy Act exemption claimed for their systems of records?[74]

12f. Does the agency's Privacy Program Page include a list and provide links to all Privacy Act implementation rules promulgated pursuant to 5 U.S.C. § 552a(f)?[75]

12g. Does the agency's Privacy Program Page include a list and provide links to all publicly available agency policies on privacy, including any directives, instructions, handbooks, manuals, or other guidance?[76]

12h. Does the agency's Privacy Program Page include a list and provide links to all publicly available agency reports on privacy?[77]

12i. Does the agency's Privacy Program Page include instructions in clear and plain language for individuals who wish to request access to or amendment of their records pursuant to 5 U.S.C. § 552a(d)?[78]

12j. Does the agency's Privacy Program Page include appropriate agency contact information for individuals who wish to submit a privacy-related question or complaint?[79]

12k. Does the agency's Privacy Program Page identify the agency's SAOP and include appropriate contact information for his or her office?[80]

---

[1] The term "information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. *See* 44 U.S.C. § 3502(8). The term "information resources" means information and related resources, such as personnel, equipment, funds, and information technology. *See* 44 U.S.C. § 3502(6). The term "Federal information system" means an information system used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency. *See* OMB Circular A-130, Managing Information as a Strategic Resource, § 10(a)(23) (July 28, 2016).
[2] The term "personally identifiable information" means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. *See* OMB Circular A-130, Managing Information as a Strategic Resource, § 10(a)(57) (July 28, 2016).
[3] The term "information technology" means any equipment, software or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. *See* OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 26, 2003).
[4] Agencies are required to update PIAs whenever changes to the information technology, changes to the agency's practices, or other factors alter the privacy risks associated with the use of such information technology. For the

purposes of this question, an up-to-date PIA is a PIA that reflects any changes to the information technology, changes to the agency's practices, or other factors that altered the privacy risks associated with the use of such information technology. *See* OMB Circular A-130, Managing Information as a Strategic Resource, Appendix II § 5(e) (July 28, 2016).

[5] The term "system of records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. *See* 5 U.S.C. § 552a(5).

[6] Agencies are required to publish a SORN in the *Federal Register* when establishing a new system of records and must also publish notice in the *Federal Register* when making significant changes to an existing system of records. For the purposes of this question, an up-to-date SORN is a published SORN that reflects any significant changes that have been made to the system of records. *See* OMB Circular A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act (Dec. 2016).

[7] *See* OMB Memorandum M-16-24, Role and Designation of Senior Agency Officials for Privacy (Sept. 15, 2016).

[8] The role and requirements for the SAOP are described in OMB guidance. *See* OMB Memorandum M-16-24, Role and Designation of Senior Agency Officials for Privacy (Sept. 15, 2016).

[9] *See id.*

[10] Agencies are required to develop and maintain a privacy program plan that provides an overview of the agency's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the SAOP and other privacy officials and staff, the strategic goals and objectives of the privacy program, the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks, and any other information determined necessary by the agency's privacy program. *See* OMB Circular A-130, Managing Information as a Strategic Resource, Appendix I § 4(c)(2), 4(e)(1) (July 28, 2016).

[11] *See* OMB Circular A-130, Managing Information as a Strategic Resource, § 5(f)(1)(j) (July 28, 2016).

[12] *See* OMB Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies (June 25, 2010).

[13] *See id.*

[14] *See* OMB Circular A-130, Managing Information as a Strategic Resource, § 5(a)(1)(a)(ii), 5(f)(1)(e) (July 28, 2016).

[15] *See id.*

[16] *See id* at § 5(f)(1)(d).

[17] Agencies are not required to have an inventory of collection and use of SSNs. However, agencies need to have a sufficient evidentiary basis to determine whether they have met the requirement to eliminate unnecessary collection and use of SSNs. *See* OMB Circular A-130, Managing Information as a Strategic Resource, § 5(f)(1)(f) (July 28, 2016).

[18] Agencies are required to take steps to eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to the use of Social Security numbers as a personal identifier. *See* OMB Circular A-130, Managing Information as a Strategic Resource, § 5(f)(1)(f) (July 28, 2016).

[19] *See* OMB Circular A-130, Managing Information as a Strategic Resource, Appendix I § 4(b)(1) (July 28, 2016).

[20] *See id.* at § 5(d)(3).

[21] *See id.* at § 5(a)(3)(e)(ii).

[22] *See id.* at Appendix I § 4(b)(3).

[23] *See id.* at Appendix I § 3(b)(10).

[24] *See id.* at § 5(a)(1)(b)(ii), Appendix I § 4(j)(1).

[25] *See id.* at Appendix I § 4(j)(3).

[26] *See id.* at Appendix I § 4(j)(2)(a).

[27] *See id.* at Appendix I § 4(h)(1)-(2), (4)-(7).

[28] *See id.* at Appendix II § 5(e).

[29] *See id.*

[30] *See id.*

[31] *See id.*

[32] *See id.*

[33] *See id.*

[34] *See id.* at § 5(c)(2).

[35] *See id.* at § 5(c)(6).

[36] *See id.* at § 5(c)(1).

[37] *See id.*

[38] *See id.* at Appendix I § 4(h)(1).

[39] *See id.* at Appendix I § 4(h)(4).
[40] *See id.*
[41] *See id.* at Appendix I § 4(h)(5).
[42] *See id.* at Appendix I § 3(b)(9).
[43] *See id.* at Appendix I § 4(h)(6).
[44] *See id.* at Appendix I § 4(h)(7).
[45] *See* OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, § VII, XI (Jan. 3, 2017).
[46] *See id.* at § X.B, XI.
[47] *See id.* at § VII.A, XI.
[48] *See id.* at § X.A, XI.
[49] *See id.* at § III.C, XI.
[50] *See id.* at § VII.D.1, XI.
[51] *See id.* at § VII.D.3, XI.
[52] *See id.* at § XI.
[53] *See* OMB Circular A-130, Managing Information as a Strategic Resource, Appendix I § 3(a), 3(b)(5) (July 28, 2016).
[54] *See id.* at Appendix I § 4(a)(2), 4(e)(7).
[55] *See id.* at Appendix I § 4(e)(5); *see also id.* at § 10(a)(14), (26), (66) and (86).
[56] Agencies shall develop and maintain a privacy plan that details the privacy controls selected for an information system that are in place or planned for meeting applicable privacy requirements and managing privacy risks, details how the controls have been implemented, and describes the methodologies and metrics that will be used to assess the controls. *See* OMB Circular A-130, Managing Information as a Strategic Resource, Appendix I § 4(c)(9), (e)(8) (July 28, 2016).
[57] *See id.* at Appendix I § 4(3).
[58] The SAOP shall develop and maintain a privacy continuous monitoring strategy, a formal document that catalogs the available privacy controls implemented at the agency across the agency risk management tiers and ensures that the privacy controls are effectively monitored on an ongoing basis by assigning an agency-defined assessment frequency to each control that is sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks. *See* OMB Circular A-130, Managing Information as a Strategic Resource, Appendix I § 4(d)(9), 4(e)(2) (July 28, 2016).
[59] The SAOP shall establish and maintain an agency-wide privacy continuous monitoring program that implements the agency's privacy continuous monitoring strategy and maintains ongoing awareness of threats and vulnerabilities that may pose privacy risks; monitors changes to information systems and environments of operation that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII; and conducts privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented at the agency across the agency risk management tiers to ensure continued compliance with applicable privacy requirements and manage privacy risks. *See* OMB Circular A-130, Managing Information as a Strategic Resource, Appendix I § 4(d)(10)-(11), 4(e)(2) (July 28, 2016).
[60] *See* OMB Circular A-130, Managing Information as a Strategic Resource, Appendix I § 4(e)(9) (July 28, 2016).
[61] *See* 5 U.S.C. § 552a(e)(4).
[62] *See id.* at § 552a(e)(3).
[63] *See id.* at § 552a(d).
[64] *See* OMB Circular A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act, § 12(a) (Dec. 2016).
[65] *See id.* at § 12(b).
[66] *See id.* at § 12(c).
[67] *See id.* at § 12(d).
[68] *See id.* at § 12(e).
[69] *See id.* at § 12(f).
[70] *See* OMB Memorandum M-17-06, Policies for Federal Agency Public Websites and Digital Services, § 6(A) (Nov. 8, 2016).
[71] *See id.* at § 6(A)(1)(a).
[72] *See id.* at § 6(A)(1)(b).
[73] *See id.* at § 6(A)(1)(c).
[74] *See id.* at § 6(A)(1)(d).
[75] *See id.* at § 6(A)(1)(e).
[76] *See id.* at § 6(A)(1)(f).

[77] *See id.* at § 6(A)(1)(g).
[78] *See id.* at § 6(A)(1)(h).
[79] *See id.* at § 6(A)(1)(i).
[80] *See id.* at § 6(A)(1)(j).